UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

BRANDON DURHAM, individually and on behalf of all those similarly situated, Plaintiff, v. BRIGHTON-BEST INTERNATIONAL, Defendant.	**No. 1:23-cv-3221** **Class Action** **Jury Trial Demanded**

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Brandon Durham ("Durham" or "Plaintiff") brings this Class Action Complaint and Demand for Jury Trial against Defendant Brighton Best International, Inc. ("Brighton" or "Defendant") to put a stop to its unlawful collection, use, and storage of Plaintiff's and the putative Class members' sensitive biometric data. Plaintiff, for his Class Action Complaint, alleges as follows upon personal knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief.

NATURE OF THE ACTION

1. Defendant Brighton operates in the tool and fastener industry, distributing such products as hand tools, socket products, nuts, washers, screws, and other products. It operates from over 30 different locations in 6 countries globally and has over 7,000 distributors for its products throughout the world. Its global headquarters are located in Tainan, Taiwan.

2. When employees first begin their jobs at Brighton, they are required to scan their fingerprint in its biometric time tracking system as a means of authentication, instead of using only

key fobs or other identification cards.

3. While many employers use conventional methods for tracking time worked (such as ID badge swipes or punch clocks), Brighton employees are required to have their fingerprint scanned by biometric timekeeping device.

4. While there are benefits to using biometric time clocks in the workplace, there are also serious risks. Unlike key fobs or identification cards—which can be changed or replaced if stolen or compromised—fingerprints are unique, permanent biometric identifiers associated with the employee. This exposes Defendant's employees to serious and irreversible privacy risks. For example, if a fingerprint database is hacked, breached, or otherwise exposed, employees have no means by which to prevent identity theft and unauthorized tracking. For example, if a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Yahoo, eBay, Equifax, Uber, Home Depot, MyFitnessPal, Panera, Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels, and Facebook/Cambridge Analytica data breaches or misuses – employees have no means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

5. In 2015, a data breach at the United States Office of Personnel Management exposed the personal identification information, including biometric data, of over 21.5 million federal employees, contractors, and job applicants. U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018), *available at* https://www.opm.gov/cybersecurity/cybersecurity-incidents.

6. A black market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including fingerprints, iris scans, and a facial photograph – of over a billion Indian citizens. *See* Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity*

Theft, The Washington Post (Jan. 4, 2018), *available at* https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c702759f138.

7. In January 2018, an Indian newspaper reported that the information housed in Aadhaar was available for purchase for less than $8 and in as little as 10 minutes. Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, The Tribune (Jan. 4, 2018), *available at* http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

8. Recognizing the need to protect its citizens from these situations, the State of Illinois enacted the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA") in 2008, specifically to regulate companies that collect and store Illinois citizens' biometrics, such as fingerprints.

9. Despite this law, Brighton disregards its employees' statutorily protected privacy rights and unlawfully collects, stores, and uses their biometric data in violation of the BIPA. Specifically, Brighton has violated (and continues to violate) the BIPA because it did not:

- Properly inform Plaintiff and the Class members in writing of the specific purpose and length of time for which their fingerprints were being collected, stored, and used, as required by the BIPA;
- Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff and the Class's fingerprints, as required by the BIPA; nor
- Receive a written release from Plaintiff or the members of the Class to collect, capture, or otherwise obtain fingerprints, as required by the BIPA.

10. Accordingly, this Complaint seeks an order: (1) declaring that Defendant's conduct violates the BIPA; (2) requiring Defendant to cease the unlawful activities discussed herein; and (3) awarding liquidated damages to Plaintiff and the proposed Class.

PARTIES

11. Plaintiff Brandon Durham is a natural person and citizen of the State of Illinois.

12. Defendant Brighton is a California corporation with its global headquarters in Tainan, Taiwan and its U.S. Headquarters in Long Beach, California. Its Illinois warehouse and offices are located at 940 North Enterprise Street, Aurora, Illinois 60504. Brighton conducts business throughout this District, in the State of Illinois, and the United States.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(a)(1) because the parties are citizens of different states and the amount in controversy exceeds $75,000, exclusive of interest and costs. This Court also has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest or costs; there are more than 100 members in the proposed class; and at least one member of the class are citizens of a state different from Defendant.

14. This Court has personal jurisdiction over Defendant because Defendant is authorized to conduct and do business in Illinois, including this District. Defendant has sufficient minimum contacts with this State and/or has sufficiently availed itself of the markets in this State to render the exercise of jurisdiction by this Court permissible.

15. Venue is proper in this District under 28 U.S.C. § 1391 (a) and (b) because a substantial part of the events giving rise to Plaintiff's claim occurred while he resided in this District.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

16. In the early 2000's, major national corporations started using Chicago and other locations in Illinois to test "new [consumer] applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school

cafeterias." 740 ILCS 14/5(b). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing, yet unregulated technology. *See* 740 ILCS 14/5.

17. In late 2007, a biometrics company called Pay By Touch—which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions—filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records—which, are unique biometric identifiers, can be linked to people's sensitive financial and personal data—could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who had used that company's fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that unique biometric identifiers could now be sold to unknown third parties.

18. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted the BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS 14/5.

19. BIPA is an informed consent statute which achieves its goal by making it unlawful for a company to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it *first*:

> (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or

biometric information.

740 ILCS 14/15(b).

20. BIPA specifically applies to employees who work in the State of Illinois. BIPA defines a "written release" specifically "in the context of employment [as] a release executed by an employee as a condition of employment." 740 ILCS 14/10.

21. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and face geometry, and—most importantly here—fingerprints. *See* 740 ILCS 14/10. Biometric information is separately defined to include any information based on an individual's biometric identifier that is used to identify an individual. *See id.*

22. BIPA also establishes standards for how employers must handle Illinois employees' biometric identifiers and biometric information. *See* 740 ILCS 14/15(c)–(d). For instance, BIPA requires companies to develop and comply with a written policy—made available to the public—establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting such identifiers or information has been satisfied or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS 14/15(a).

23. Ultimately, BIPA is simply an informed consent statute. Its narrowly tailored provisions place no absolute bar on the collection, sending, transmitting or communicating of biometric data. For example, the BIPA does not limit what kinds of biometric data may be collected, sent, transmitted, or stored. Nor does the BIPA limit to whom biometric data may be collected, sent, transmitted, or stored. The BIPA simply mandates that entities wishing to engage in that conduct must make proper disclosures and implement certain reasonable safeguards.

II. Brighton Violates the Illinois Biometric Information Privacy Act.

24. By the time the BIPA passed through the Illinois Legislature in mid-2008, many

companies who had experimented with using biometric data as an authentication method stopped doing so, at least for a time. That is because Pay By Touch's bankruptcy, described in Section I above, was widely publicized and brought attention to consumers' discomfort with the use of their biometric data.

25. Unfortunately, Brighton specifically failed to take note of the passage of the BIPA. Brighton continues to collect, store, and use its employees' biometric data in violation of the BIPA.

26. Specifically, when employees work at Brighton, they are required to have their fingerprints scanned in order to enroll them in its fingerprint database.

27. Brighton uses an employee time tracking system that requires employees to use their fingerprints as a means of authentication. Unlike a traditional time clock, employees have to use their fingerprint to "punch" in to or out of work.

28. Brighton failed to inform its employees of the complete purposes for which it collects their sensitive biometric data or to whom the data is disclosed, if at all.

29. Brighton similarly failed to provide its employees with a written, publicly available policy identifying its retention schedule, and guidelines for permanently destroying its employees' fingerprints when the initial purpose for collecting or obtaining their fingerprints is no longer relevant, as required by the BIPA. An employee who leaves the company does so without any knowledge of when their biometric identifiers will be removed from Brighton databases—or if they ever will be.

30. The Pay By Touch bankruptcy that catalyzed the passage of the BIPA highlights why conduct such as Brighton —whose employees are aware that they are providing biometric identifiers but are not aware of to whom or the full extent of the reasons they are doing so—is so dangerous. That bankruptcy spurred Illinois citizens and legislators to realize a critical point: it is crucial for people to understand when providing biometric data who exactly is collecting it, who

it will be transmitted to, for what purposes, and for how long. But Brighton disregards these obligations, and instead unlawfully collects, stores, and uses its employees' biometric identifiers and information without proper consent.

31. Ultimately, Brighton disregards its employees' statutorily protected privacy rights by violating the BIPA.

FACTS SPECIFIC TO PLAINTIFF DURHAM

32. Plaintiff Durham works for Brighton at its Aurora, Illinois location from June 2022 to the present.

33. As an employee, Brighton collected the Plaintiff's fingerprint by requiring Plaintiff to scan his fingerprint so that it could use it as an authentication method to track time. Brighton subsequently stored Plaintiff's fingerprint data in its database.

34. Each time Plaintiff began and ended a workday, Brighton required a scan of Plaintiff's fingerprints. Plaintiff estimates he has scanned his fingerprint over 500 times during the time he has worked at Brighton.

35. Brighton never informed Plaintiff of the specific limited purposes or length of time for which it collected, stored, or used fingerprints.

36. Similarly, Brighton never informed Plaintiff of any biometric data retention policy it developed, nor whether it will ever permanently delete fingerprints.

37. Plaintiff never signed a written release allowing Brighton to collect or store fingerprints.

38. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Brighton violations of the BIPA alleged herein.

39. Defendant's failure to develop, publicly disclose, and comply with a data-retention schedule and guidelines for the permanent destruction of biometric data when the initial purpose

for collection ended caused injuries to Plaintiff and the Class member.

40. Plaintiff now seeks liquidated damages under BIPA as compensation for the injuries Brighton has caused.

CLASS ALLEGATIONS

41. **Class Definition**: Plaintiff Durham brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of himself and a Class of similarly situated individuals, defined as follows:

> All residents of the State of Illinois who had their fingerprints collected, captured, received, otherwise obtained, or disclosed by Brighton while residing in Illinois since March 29, 2022.

The following people are excluded from the Class: (1) any Judge presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and its current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

42. **Numerosity**: The exact number of Class members is unknown to Plaintiff at this time, but it is clear that individual joinder is impracticable. Defendant has collected, captured, received, or otherwise obtained biometric identifiers or biometric information from at least hundreds of employees who fall into the definition of the Class. Ultimately, the Class members will be easily identified through Defendant's records.

43. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class

include, but are not necessarily limited to the following:

a) whether Defendant collected, captured, or otherwise obtained Plaintiff's and the Class' biometric identifiers or biometric information;

b) whether Defendant properly informed Plaintiff and the Class of its purposes for collecting, using, and storing their biometric identifiers or biometric information;

c) whether Defendant obtained a written release (as defined in 740 ILCS 14/10) to collect, use, and store Plaintiff and the Class' biometric identifiers or biometric information;

d) whether Defendant has sold, leased, traded, or otherwise profited from Plaintiff and the Class's biometric identifiers or biometric information;

e) whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied owithin three years of their last interaction, whichever occurs first;

f) whether Defendant complies with any such written policy (if one exists); and

g) whether Defendant used Plaintiff and the Class' fingerprints to identify them.

44. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class and have retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor their counsel have any interest adverse to those of the other members of the Class.

45. **Appropriateness**: This class action is appropriate for certification because class proceedings are superior to all others available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. The damages suffered by the individual members of the Class are likely to have been small relative to the burden and

expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in their Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

FIRST CAUSE OF ACTION
Violation of BIPA Section 15(a): Failure to Institute, Maintain and Adhere to Publicly-Available Retention Schedule

46. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

47. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention – and, importantly, deletion – policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a).

48. Defendant fails to comply with these BIPA mandates.

49. Defendant is an entity registered to do business in Illinois and thus qualifies as a "private entity" Under BIPA. *See* 740 ILCS 14/10.

50. Plaintiffs are individuals who had their "biometric identifiers" (in the form of their fingerprints) collected by Defendant, as explained in detail above, *supra*. *See* 740 ILCS 14/10.

51. Plaintiff's biometric identifiers were used to identify them and, therefore, constitute

"biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

52. Defendant failed to provide a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS 14/15(a).

53. Upon information and belief, Defendant lacked retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data and have not and will not destroy Plaintiff's and the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company.

54. On behalf of themselves and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring each Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

SECOND CAUSE OF ACTION
Violation of BIPA Section 15(b): Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information

55. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

56. BIPA requires companies to obtain informed written consent from employees before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject…in

writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject…in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information…" 740 ILCS 14/15(b) (emphasis added).

57. Defendant fails to comply with these BIPA mandates.

58. Defendant is an entity registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

59. Plaintiff is an individual who had "biometric identifiers" (in the form of fingerprints) collected by Defendant, as explained above. *See* 740 ILCS 14/10.

60. Plaintiff's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

61. Defendant systematically and automatically collected, used, stored, and disclosed Plaintiff's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

62. Defendant did not inform Plaintiff in writing that their biometric identifiers and/or biometric information were being collected, stored, used, and disseminated, nor did Defendant inform Plaintiff in writing of the specific purpose and length of term for which biometric identifiers and/or biometric information were being collected, stored, used and disseminated as required by 740 ILCS 14/15(b)(1)-(2).

63. By collecting, storing, and using Plaintiff's and the Class's biometric identifiers and biometric information as described herein, each Defendant violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

64. On behalf of themselves and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring each Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

THIRD CAUSE OF ACTION
Violation of BIPA Section 15(d): Disclosure of Biometric Identifiers and Information Before Obtaining Consent

65. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

66. BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

67. Defendant fails to comply with this BIPA mandate.

68. Defendant is an entity registered to do business in Illinois and thus qualifies as a "private entity" Under BIPA. *See* 740 ILCS 14/10.

69. Plaintiff is an individual who had their "biometric identifiers" (in the form of their fingerprints) collected by Defendants, as explained in detail in Sections II and III, *supra*. *See* 740 ILCS 14/10.

70. Plaintiff's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

71. Upon information and belief, by utilizing a biometric time clock, Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated Plaintiff's

biometric identifiers and/or biometric information to at least the payroll company hired by the Defendant without first obtaining the consent required by 740 ILCS 14/15(d)(1).

72. By disclosing, redisclosing, or otherwise disseminating Plaintiff's and the Class's biometric identifiers and biometric information as described herein, each Defendant violated

Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

73. On behalf of themselves and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring each Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

74. The BIPA requires companies to obtain informed written consent from employees before acquiring their biometric data. Specifically, the BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless [the entity] first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; *and* (3) receives a written release executed by the subject of the biometric identifier or biometric information…." 740 ILCS 14/15(b) (emphasis added).

75. The BIPA also mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention (and—importantly—deletion) policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (*i.e.,* when the

employment relationship ends); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a).

76. Unfortunately, Brighton fails to comply with these BIPA mandates.

77. Brighton is a corporation and thus qualifies as a "private entity" under the BIPA. *See* 740 ILCS 14/10.

78. Plaintiff and the Class are individuals who had their "biometric identifiers" collected by Brighton (in the form of their fingerprints), as explained in detail in Section II. *See* 740 ILCS 14/10.

79. Plaintiff and the Class members' biometric identifiers or information based on those biometric identifiers were used to identify them, constituting "biometric information" as defined by the BIPA. *See* 740 ILCS 14/10.

80. Brighton violated 740 ILCS 14/15(b)(3) by negligently failing to obtain written releases from Plaintiff and the Class before it collected, used, and stored their biometric identifiers and biometric information.

81. Brighton violated 740 ILCS 14/15(b)(1) by negligently failing to inform Plaintiff and the Class in writing that their biometric identifiers and biometric information were being collected and stored.

82. Brighton violated 740 ILCS 14/15(b)(2) by negligently failing to inform Plaintiff and the Class in writing of the specific purpose and length of term for which their biometric identifiers or biometric information was being collected, stored, and used.

83. Brighton violated 740 ILCS 14/15(a) by negligently failing to publicly provide a retention schedule or guideline for permanently destroying its employees' biometric identifiers and biometric information.

84. By negligently collecting, storing, and using Plaintiff's and the Class' biometric

identifiers and biometric information as described herein, Brighton violated Plaintiff's and the Class' rights to privacy in their biometric identifiers or biometric information as set forth in the BIPA, 740 ILCS 14/1, *et seq*.

85. On behalf of themselves and the Class, Plaintiff seek: (1) injunctive and equitable relief as is necessary to protect the interests of the Plaintiff and the Class by requiring Defendant to comply with the BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (2) liquidated damages of $1,000 per violation for each of Defendant's negligent violations of the BIPA pursuant to 740 ILCS 14/20(1); and (3) reasonable attorneys' fees and costs and expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Brandon Durham, on behalf of himself and the Class, respectfully request that the Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Durham as representative of the Class, and appointing their counsel as Class Counsel;

B. Declaring that Defendant's actions, as set out above, violate the BIPA;

C. Awarding damages for each of Defendant's violations of the BIPA, pursuant to 740 ILCS 14/20;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including an Order requiring Defendant to collect, store, and use biometric identifiers or biometric information in compliance with the BIPA;

E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys'

fees;

F. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

G. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated: May 22, 2023

Respectfully submitted,

Brandon Durham individually and on behalf of all others similarly situated,

By: /s/Keith L. Gibson
One of Plaintiff's Attorneys

Keith L. Gibson, Esq.
IL Bar No.: 6237159
490 Pennsylvania Avenue, Suite 1
Glen Ellyn IL 60137
Telephone: (630) 677-6745
Email: keith@keithgibsonlaw.com

Bogdan, Enica, Esq.
Law Offices of Keith L. Gibson
FL Bar No.: 101934
66 West Flagler St., Ste. 937
Miami, FL 33130
Telephone: (305) 539-9206
Email: bogdan@keithgibsonlaw.com

Attorneys for the Plaintiff and the Putative Class